(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2003 (27.11.2003)

PCT

(10) International Publication Number
WO 03/098409 A1

(51) International Patent Classification⁷: G06F 1/00 // H04L 29/06

(21) International Application Number: PCT/SE03/00796

(22) International Filing Date: 16 May 2003 (16.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/381,425	17 May 2002 (17.05.2002)	US
10/438,453	14 May 2003 (14.05.2003)	US

(71) Applicant: TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors: LINDHOLM, Fredrik; Stamgatan 86, S-125 74 Älvsjö (SE). CARRARA, Elisabetta; Malmvägen 6B, S-191 61 Sollentuna (SE). JONSSON, Björn; August Plyms väg 12, S-133 33 Saltsjöbaden (SE). NERBRANT, Per-Olof; Katarinavägen 20, S-184 51 Österskär (SE).

(74) Agent: BOESTAD, Karin; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

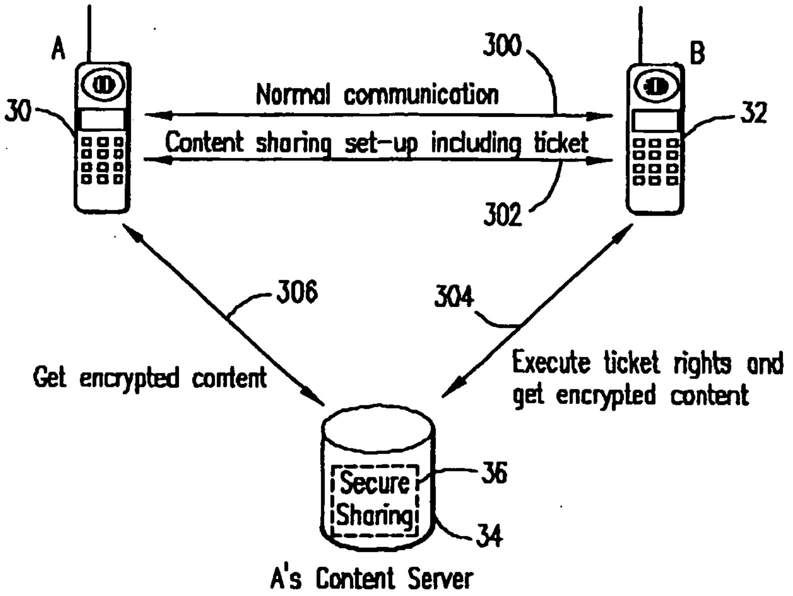
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE CONTENT SHARING IN DIGITAL RIGHTS MANAGEMENT



(57) Abstract: Method and system for securely sharing content in real-time systems over heterogeneous networks. Cryptographic mechanisms of the content are used to protect the confidentiality and the integrity of the content. The confidentiality/integrity protection may be performed either before storing the content on the content server (i.e., pre-encryption), or by the content server while the content is being sent (i.e., real-time encryption).

SECURE CONTENT SHARING IN DIGITAL RIGHTS MANAGEMENT

CROSS-REFERENCE TO RELATED APPLICATION

This application for patent claims the benefit of priority from, and hereby incorporates by reference, U.S. Provisional Patent Application Serial No. 60/381,425 entitled "SECURE CONTENT SHARING - PERSONAL DRM" filed with the U.S. Patent and Trademark Office on May 17, 2002.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to the sharing and distribution of digital content and, in particular, to a method and system for securely sharing digital content in a digital rights management (DRM) system.

Description of the Related Art

Digital content (hereinafter "content"), such as audio, video, text, data, multimedia files and the like, can be easily and often illicitly shared or distributed, usually over a computer network. As a result, DRM technology was developed to restrict the sharing or distribution of the content. For example, content that is protected by DRM technology can be limited with respect to file access (e.g., number of views, length of views), altering, sharing, copying, printing, and saving. DRM restrictions are typically implemented in two ways. First is "containment," where the content is encrypted so that only an authorized user can access it. Second is "marking," where a watermark, flag, or an XrML tag is placed on the content as a signal to a terminal that the content is copy protected. These restrictions may be implemented within the operating system, software program, or in the actual hardware of a terminal.

Such restrictions, however, can make it difficult for the owners of the DRM content to share the content. This is because DRM restrictions are typically implemented on a terminal specific basis, that is, the DRM content is authorized to and accessible by one particular terminal. If the user tries to transfer or forward the content to another terminal, the new terminal will be unable to play/view the content. Thus, the user cannot share or distribute (at least not easily) his own content or content that he has purchased. To the extent that some DRM systems do allow sharing or distribution of DRM content, the content must be shared using the method imposed by the DRM system. This restriction limits the ability of the content purchaser to select the sharing or distribution method.

There are generally two methods of sharing and distributing content, as can be seen in Figure 1. Both methods begin with the parties establishing communication with one another in step 100. The communication is typically established using some type of secure connection. Thereafter, party A decides to share her content with party B. In the first approach, party A shares her content by sending a pointer to the content to party B at step 102 . The content itself is typically stored on party A's personal content server 10, of which party A and party B are clients, but to which only party A has authorized access normally (i.e., only party A can download content to the server). Party B then uses the pointer received from party A to send a request to the content server 10 at step 104. At step 106, the content server locates the content specified by the content pointer and sends the content to party B. In this way, party B is able to obtain party A's content.

In the second approach, instead of party A sending the pointer to party B at step 102, party A instructs the content server 10 regarding which content is to be shared and with whom at step 108. In this approach, party A and party B typically have arrived at some understanding or agreement beforehand regarding sharing of the content. The content sever 10 can then be used to "push" party A's content to party B.

In both of the approaches shown in Figure 1, party A and party B are peers who can communicate with one another through their respective personal communication terminals 12 and 14, such as a mobile phone, a personal digital assistant, and the like. The communication between party A, party B, and the content server may be carried on a wireless link, a wired link, or a combination of both (e.g., one user is on a wireless link while the other user is on a wired link). Also, both party A and party B can be connected to one or more other content servers and other parties in addition to those shown in Figure 1.

The increased use and distribution of content has placed increasingly greater demands on DRM and other similar systems. For example, there is no general security architecture for sharing content in real-time systems over arbitrary or heterogeneous networks (i.e., networks involving computers with disparate software and/or hardware). Present security architectures only provide the owner of the content with access control, which is the ability to give different users/clients different levels of access to the content. A full security solution, however, should include more than just access control. Confidentiality of the parties involved and integrity protection of the content are also needed. Such security measure, however, are difficult to implement in content sharing applications that are used in real-time systems over arbitrary networks. The problem is compounded when the content is DRM content and, therefore, must be shared or distributed in the method imposed by the DRM system.

Accordingly, it would be desirable to provide a general security architecture that can be applied to content sharing applications used in real-time systems over arbitrary networks. More particularly, it would be desirable to provide a secure method and system for sharing DRM content in real-time systems over arbitrary networks.

SUMMARY OF THE INVENTION

The present invention is directed to a method and system for securely sharing content in real-time systems over arbitrary networks. The invention uses cryptographic techniques on the content to protect the confidentiality and integrity of the content shared between the parties involved. The confidentiality/integrity protection is independent of any of the underlying networks and may be performed either before storing the content on the content server (i.e., pre-encryption), or by the content server while the content is being sent (i.e., real-time encryption). Real-time encryption may be most suitable for real-time content, DRM content that may be manipulated by the content server, and content that cannot be pre-encrypted for some other reason. Pre-encryption may be most suitable for all other types of content, such as movies and music. In this way, the desired level of security, including access control, confidentiality, and integrity protection may be provided for real-time systems over arbitrary networks.

In general, in one aspect, the invention is directed to a method for sharing content between a first party and a second party in a secure communication session. The method comprises storing a content of the first party on a personal content server and distributing access information for the content from the first party to the second party, the access information allowing the second party to access the content. The method further comprises presenting the access information of the second party to the personal content server, verifying the access information from the second party in the personal content server, and processing the content for distribution to the second party upon verification of the access information.

In general, in another aspect, the invention is directed to a telecommunication system wherein content may be shared between a first party and a second party in a secure manner. The system comprises a first party terminal connected to a second party terminal in a secure communication session, the first party terminal configured to distribute access information for a content to the second party, the access information allowing the second party to access the content. The system further comprises a personal content server connected to the first and second party terminals and storing a content of the first party thereon, the personal content server configured to verify the access information when it is presented to the personal content server by the second party, and to process the content for distribution to the second party upon verification of the access information.

In general, in yet another aspect, the invention is directed to a network node for facilitating secure sharing of content between a first party and a second party. The network node normally accessible by the first party only, and comprising means for establishing a secure connection to the terminals of the first and second parties, means for storing a content of the first party, and means for issuing access authorization to the second party terminal. The network node further comprises means for receiving a request to access the content using the access authorization from the second party terminal, means for verifying the received access authorization, and means for distributing the content in a secure manner to the second party terminal upon verification of the access authorization.

It should be emphasized that the term comprises/comprising, when used in this specification, is taken to specify the presence of stated features, integers, steps, or components, but does not preclude the presence or addition of one or more other features, integers, steps, components, or groups thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

A better understanding of the invention may be had by reference to the following detailed description when taken in conjunction with the accompanying drawings, wherein:

Figure 1 illustrates an example of an existing content sharing/distribution model;

Figure 2 illustrates an exemplary content sharing/distribution model according to embodiments of the invention;

Figure 3 illustrates another exemplary content sharing/distribution model according to embodiments of the invention;

Figure 4 illustrates an exemplary DRM content sharing/distribution model according to embodiments of the invention;

Figure 5 illustrates a flowchart for an exemplary implementation for a DRM module according to embodiments of the invention;

Figure 6 illustrates a flowchart for another exemplary implementation of a DRM module according to embodiments of the invention; and

Figure 7 illustrates a flowchart for an exemplary DRM content manipulation procedure according to embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

Following is a detailed description of the invention with reference to the drawings wherein reference numerals for the same and similar elements are carried forward.

As mentioned above, embodiments of the invention provide a secure method and system for sharing content. The present invention uses cryptographic mechanisms to protect the confidentiality and the integrity of the content. The cryptography should be independent of the underlying network and robust enough to handle a wide variety of connections, including low speed connections with high error rates (e.g., dial-up connections). An example of such a cryptographic mechanism is the Secure Real-time Transport Protocol (SRTP), which can provide both confidentiality protection of the user data and integrity protection on a per packet basis. Depending on the specifics of the application, either pre-encryption or real-time encryption may be used. The latter approach is especially useful where the content owner can use a trusted server (e.g., her own server, which is located at home or at her office). In that case, the owner has complete confidence in the server and does not have to worry about confidentiality or integrity. Thus, she may not want to, or simply cannot for some other reason, have the content pre-encrypted on the server. Therefore, in accordance with embodiments of the invention, the content server encrypts the content "on-the-fly" as it is being sent to a user.

The "on-the-fly" encryption approach is illustrated in Figure 2, where two or more parties are connected together. As before, the parties may be connected through their personal communication terminals 20 and 22 via a wireless and/or a wired link. Party A is the content owner, and party B represents one or more other parties who are interested in obtaining party A's content. The parties are also connected to the party A's personal content server 24, to which only party A has authorized access normally. The personal content server 24 of party A, however, is able to accept a request for rendering of specified contents by other parties capable of presenting access rights such as a ticket. In accordance with embodiments of the invention, the personal content sever includes a secure sharing function 26 that is capable of issuing access authorization (e.g., in the form of "tickets"), verifying the access authorization, as well as encrypting the content "on-the-fly".

The first step in this approach is for the parties to establish a communication between them in step 200. The communication is again preferably carried on a secure connection. For example, a session key may be used to establish a secure connection between the parties. During the course of the communication, the parties agree to a sharing of party A's content (e.g., some pictures or a small video clip) with the other parties. Party A thereafter sends the location of the content, the security parameters, and any additional information that may be needed for security purposes to party B in step 202. The location of the content may be, for example, an HTTP, an FTP or an RTSP (Real-time Streaming Protocol) URL address. The security parameters may be sent in the form of a "ticket" or other key management protocols known to those having ordinary skill in the art, such as MIKEY (Multimedia Internet KEYing). MIKEY is a key management protocol designed to transport keys and other security parameters for different security protocols. "Tickets" are essentially electronic tokens, usually granted to authorize access to a specific resource under certain restrictions (e.g., during a certain time period or for a specific number of times).

Once the location and security information have been sent, the parties, including the content owner, initiate a secure download/streaming (e.g., using RTSP/RTP (Real-time Transport Protocol)) from the content server. This may be done in two different ways. The first approach is for party A to initiate the entire download/streaming session by sending the session information, including a key management message, to the content server 24 in step 204. The key management message includes keys that would be used by the secure sharing function 26 of the content server 24 to encrypt and protect the specific content. The content server 24 then encrypts the content and "pushes" the encrypted content to the involved parties at step 206. The encrypted content may be simultaneously pushed to multiple parties, for example, where party A has directed the content server to multicast to the parties. Party A also sends the session information to the other involved parties (step 202), including the key management message, using a key management protocol such as MIKEY. The other parties then use the keys in the key management message to decrypt the encrypted content received from the content server 24.

The second approach, illustrated in Figure 3, is to use a "ticket" approach, where each communicating party receives a "ticket" that can be shown to the content server 24. In this approach, normal communication between the parties is again established at step 300 via their respective terminals 30 and 32 using a secure connection. At step 302, the parties again agree to a sharing of party A's content, which is stored on party A's personal content server 34. In accordance with embodiments of the invention, the content server 34 includes a secure sharing function 36 that is similar to the secure sharing function 26 in the previous figure (i.e., one that is capable of issuing access authorization, verifying the access authorization, and encrypting the content while it is being distributed). Party A thereafter sends a "ticket" to party B that contains information about the content as well as security parameters. The security parameters include keys that are used by the content server to encrypt party A's content. Party B thereafter presents its ticket to the content server 34. If the secure sharing function 36 the content server 34 can validate the ticket, the encrypted content is distributed to the holders of the ticket at step 304 (using security mechanisms described in the ticket). Some key management protocols, for example, the MIKEY protocol, can with small modifications be used as a "ticket."

Note that party A may also request and receive the encrypted content at step 306. One reason for this is party A may have originally downloaded the content to her personal content server 34 in encrypted form. Thus, for party A to access the content, she would need a ticket from the content provider allowing access to the content. By presenting the ticket to the content server, party A is able to obtain and view the content in parallel with party B, which allows the two parties to discuss the content together.

In another aspect of the second approach, the ticket includes only part of a content key such as a nonce. According to this aspect, all parties share a common public function *f* which can be used to derive a content key C_k, where $C_k = f$(session key, nonce), and the session key is available only during an ongoing session. In this way, the ticket is made valid only during an ongoing session and cannot be used to obtain access to the contents in a later session.

As for the pre-encryption (and/or pre-integrity protected) approach, this approach is similar to the "on-the-fly" approach illustrated in Figure 2. The main difference is that the content is encrypted before it is placed on the content server 10 so that whatever content is stored on the content server is already encrypted. This pre-encryption relieves the burden on party A of having to use a trusted or secure content server. Instead, party A may place its encrypted content on any available server. The encryption keys may then be distributed by party A over the secure connection (step 202) to the other involved parties along with location information for the content and security parameters. The other involved parties may thereafter use the encryption keys to access and decrypt the content on the content server. This approach has the advantage of requiring almost no additional functionality on the content server, such as encryption functionality, relative to the "on-the-fly" approach.

The foregoing embodiments address the problem of content sharing/distribution in general. The sharing/distribution of DRM content, however, poses a somewhat different problem due to the terminal specific authorization of DRM technology. While some DRM systems provide a special feature for forwarding content that has been authorized for one terminal to another, typically the original terminal loses its authorization in the process so that only one terminal is enabled at any time for the particular DRM content. This problem of sharing DRM content in general has not been heretofore addressed. However, by extending the content sharing model of the present invention, the DRM content sharing problem can be solved.

The present invention solves the problem of sharing DRM content by letting the user's content server handle some of the traditional DRM functionality, such as local access and rights management control. The user's content server will also handle the main communication with the DRM content server. Thus, instead of buying DRM content for a specific terminal, a user can buy the DRM content for her personal content server. The personal content server can then re-distribute the DRM content to the user's other terminals. This will make it easier for the user to view the content on different DRM enabled terminals, and also to share the content with other users in a restricted and controlled manner.

Figure 4 illustrates a method of sharing/distributing DRM content according to embodiments of the invention. As can be seen, two or more parties are connected together, as before, through their personal communication terminals 40 and 42 via a wireless and/or a wired link. Party A is the party that has legally purchased one or more DRM content, and party B represents one or more other parties who are interested in obtaining party A's DRM content. The parties are also connected to party A's personal content server 44, which is a DRM content server, via the wireless and/or wired link. The terminals 40 and 42 and the personal content server 44 in Figure 4 are slightly different from their counterparts in the previous figures in that they each contain a DRM module (only the DRM module 46 of the server 44 is shown here). The DRM module is the mechanism that either allows or prohibits playing/viewing of DRM protected content on a terminal according to whether the terminal was enabled for that content. Such DRM modules are known to those having ordinary skill in the art and may be implemented as software, hardware, or a combination of both.

In accordance with embodiments of the invention, the DRM module 46 of the personal content server 44 also allows it to perform certain traditional DRM functionality. For example, the personal content sever 20 is able to perform verification of access rights and to modify those access rights. Thus, the personal content sever 20 is able to verify party A's access rights and, where sharing is appropriate, transfer a certain amount of those access rights to a ticket that is distributed to party B for shared access to the content. In some embodiments, the personal content sever 20 is able to modify the content itself, for example, by reformatting the content, re-encrypting the content, and marking the content. The personal content sever 20 is also able to verify whether a DRM module exists in the terminals of each involved party and whether the modules, including the server's own DRM module, is valid and up to date.

A DRM content provider 48 is connected to the personal content server 44 and is responsible for storing and providing DRM protected content to legal purchasers of the content such as the personal content server 44. The DRM content provider 48 is, in turn, connected to a DRM authority 50. The DRM authority 50 handles the issuing of rights (i.e., the tickets) to specific DRM protected content for a purchaser and his terminal devices. The DRM authority 50 may also handle financial functions, such as the charging and billing of the purchaser. The DRM content provider 48 accepts tickets issued by the DRM authority 50, and also provides the content according to the rules set in the ticket.

As in previous embodiments, the first step in Figure 4 is for the parties to establish a secure communication between them at step 400 using, for example, a session key. Then, when party A attempts to share a DRM protected content, party A's content server 44 first verifies at step 402 that the terminals of all involved parties, including party A's terminal, contains a valid DRM module, either as software or hardware. The personal content server 44 also has its own DRM module that it must verify. The personal content server 44 performs this verification by obtaining information (e.g., identification, status, etc.) regarding each DRM module and confirming with the DRM authority 50 whether the DRM module is valid. Since the DRM authority 50 is the entity that issues and revokes DRM modules, it is the entity that can properly authenticate a DRM module. Note that this arrangement requires some type of existing relationship (indicated by the dotted arrow) between the DRM content provider 48 and the DRM authority 50 (e.g., one may be owned by the other).

Once the personal content server 44 verifies that all involved parties have a valid DRM module, it verifies (again at step 402) that party A has the right to access and to share DRM content with other terminals. After this verification, the personal content server 44 obtains at step 404 the DRM protected content from the DRM content provider 48. Thereafter, each time one of the parties requests the DRM protected content, the personal content server 44 can reacquire the content from the DRM content provider 48, or it can store a copy of the content locally for subsequent access.

The right to access and to share DRM content can be very flexible. For example, the buyer can be allowed to share the entire content, parts of the content, the entire content a specific number of times, and other similar arrangements. The content can then be distributed to the different parties using the approach described previously in Figures 2-3. The particular method used will depend on whether party A's personal content server 44 has the right to manipulate the content or it if is only allowed to forward the content. Where the personal content server 44 includes only a DRM module 46 that does not allow to manipulation of the content from the DRM content provider 48. In that case, the personal content server 44 will distribute the content in a manner very similar to the pre-encrypted distribution model discussed above.

If, on the other hand, the personal content server 44 includes a DRM module 46 that allows manipulation of the DRM content, then a different approach may be used. For example, the DRM module may be used to re-encrypt, watermark, and re-format the DRM content in a secure way so that the content fits the terminals that it is sent. The distribution principle used in this scenario is then very similar to the "on-the-fly" distribution model discussed earlier. In some embodiments, it is possible for the DRM module in the terminal of party A to issue the encryption key for the content. That key will then be used to re-encrypt the content in the manipulation process of the personal content server 44. The same key is distributed to the other involved parties.

In some embodiments, the personal content server's DRM module 46 can create a software DRM module for transfer and download into a terminal. In this way, the personal content server's DRM module and the terminal located DRM modules may be made to match one another. Furthermore, the server and terminal implemented DRM modules may contain a function *f* that can be used to derive a content key C_k and an address to the content server. The derivation may use a nonce and a session identity, as described in above with respect to the "ticket" approach.

Figure 5 illustrates a flow diagram 500 that represents one exemplary implementation of a DRM module in the personal content server where no manipulation of content is allowed. As can be seen, the first thing that the server DRM module does is verify that the client or terminal DRM modules are valid at step 502. This verification can be done, for example, via the DRM authority described above. If the verification fails (i.e., one or more of the terminal DRM modules are invalid), then the server DRM module returns to the beginning of the flow diagram. Otherwise, at step 504, the server DRM module obtains the desired DRM protected content, either from a DRM content provider or from a locally stored copy of the content. The server DRM module thereafter verifies that the purchasing party has distribution rights at step 506. It may be that the purchasing party only recently purchased the distribution rights, in which case the server DRM module also update that party's rights information. Thereafter, the server DRM module continues to the distribution stage of the procedure at step 508. On the other hand, if the purchasing party has no distribution rights, then from step 506, the server DRM module returns to the beginning of the procedure.

Figure 6 illustrates a flow diagram 600 that represents one exemplary implementation of a DRM module in the personal content sever where manipulation of the content is allowed. The flow diagram 600 has essentially the same first three steps as the flow diagram 500, namely, verification of the terminal DRM modules (step 602), acquisition of the DRM protected content (step 604), and verification of distribution rights (step 606). At step 608, however, the server DRM module is allowed to manipulate the DRM protected content, as will be described further below. After manipulation, the server DRM module continues to the distribution stage of the procedure at step 610.

Figure 7 illustrates a flow diagram 700 that represents one exemplary implementation of the manipulation process (step 608). As can be seen, in some embodiments, manipulation begins with decryption of the DRM content at step 700 using the encryption key that was provided by the DRM content provider upon purchase of the DRM content. At step 702, reformatting of the content takes place if necessary for the terminal of the purchasing party or any of the involved parties to be able to use the content. After reformatting, the content is tagged or individualized with a watermark at step 704 in accordance with conventional DRM technology. The content is then re-encrypted at step 706 using either the same encryption key as before, or a separate key for some or all of the parties receiving the content. On the other hand, if no reformatting of the content is needed, then the DRM content is simply re-encrypted at step 706 without individualization at step 704.

While particular embodiments and applications of the present invention have been illustrated and described, it is to be understood that the invention is not limited to the precise construction and compositions disclosed herein, and that modifications and variations may be made to the foregoing without departing from the scope of the invention as defined in the appended claims.

CLAIMS

What is claimed is:

1. A method for sharing content between a first party and a second party in a secure communication session, comprising:

storing a content of the first party on a personal content server;

distributing access information for the content from the first party to the second party, the access information allowing the second party to access the content;

presenting the access information of the second party to the personal content server;

verifying the access information from the second party in the personal content server; and

processing the content for distribution to the second party upon verification of the access information.

2. The method according to claim 1, wherein the content comprises a streamed content, including a RTSP/RTP streamed content, and the step of processing comprises encrypting the content while it is being streamed.

3. The method according to claim 2, wherein the content may be accessed by using a ticket.

4. The method according to claim 2, wherein the streamed content is DRM protected content.

5. The method according to claim 4, wherein the personal content server is capable of manipulating the DRM content for the second party, further comprising the steps of:

authenticating a DRM module in a terminal of the second party;

confirming a right of the first party to distribute the DRM content;

manipulating the DRM content, if needed, to match the terminal of the second party; and

creating a right specifically for the second party to access the manipulated content.

6. The method according to claim 5, wherein the step of manipulating comprises

decrypting the DRM content;

reformatting the DRM content, if needed, to match the terminal of the second party;

tagging the DRM content for the terminal of the second party; and

re-encrypting the content with a specific key for the second party.

7. The method according to claim 4, wherein the personal content server has a pre-installed first DRM module and wherein the step of distributing comprises the steps of:

generating a second DRM module in the personal content server; and

distributing the second DRM module from the personal content server to the second party.

8. The method according to claim 1, wherein the personal content server and each terminal of the parties share a predetermined function, further comprising the step of:

distributing a nonce from the personal content server to the terminals; and

deriving a content key in the terminals and the personal content server based on the predetermined function, the nonce, and a session identity.

9. The method according to claim 1, wherein the content is encrypted prior to being stored on the personal content server.

10. A telecommunication system wherein content may be shared between a first party and a second party in a secure manner, comprising:

a first party terminal;

a second party terminal connected to the first party terminal in a secure communication session, the first party terminal configured to distribute access information for a content to the second party, the access information allowing the second party to access the content;

a personal content server connected to the first and second party terminals and storing a content of the first party thereon, the personal content server configured to verify the access information when it is presented to the personal content server by the second party, and to process the content for distribution to the second party upon verification of the access information.

11. The telecommunication system according to claim 10, wherein the content comprises a streamed content, including a RTSP/RTP streamed content, and the personal content server processes the content by encrypting the content while it is being streamed.

12. The telecommunication system according to claim 11, wherein the content may be accessed by using a ticket.

13. The telecommunication system according to claim 11, wherein the streamed content is DRM protected content.

14. The telecommunication system according to claim 13, wherein the personal content server is further configured to authenticate a DRM module in the second party terminal, confirm a right of the first party terminal to distribute the

DRM content, manipulate the DRM content, if needed, to match the second party terminal, and create a right specifically for the second party terminal to access the manipulated content.

15. The telecommunication system according to claim 14, wherein the personal content server manipulates the content by decrypting the DRM content, reformatting the DRM content, if needed, to match the second party terminal, tagging the DRM content for the second party terminal, and re-encrypting the content with a specific key for the second party terminal.

16. The telecommunication system according to claim 13, wherein the personal content server has a pre-installed first DRM module and is further configured to generate a second DRM module, and to distribute the second DRM module to the second party terminal.

17. The telecommunication system according to claim 10, wherein the personal content server and first and second party terminals share a predetermined function and the personal content server is configured to distribute a nonce to the terminals, and both the personal content server and the terminals are configured to derive a content key based on the predetermined function, the nonce, and a session identity.

18. The telecommunication system according to claim 10, wherein the content is encrypted prior to storage on the personal content server.

19. A network node for facilitating secure sharing of content between a first party and a second party, said network node normally accessible by the first party only, comprising:

means for establishing a secure connection to the terminals of the first and second parties;

means for storing a content of the first party;

means for issuing access authorization to the second party terminal;

means for receiving a request to access the content using the access authorization from the second party terminal;

means for verifying the received access authorization; and

means for distributing the content in a secure manner to the second party terminal upon verification of the access authorization.

20. The network node according to claim 19, wherein the content comprises a streamed content, including a RTSP/RTP streamed content, and the personal content server processes the content by encrypting the content while it is being streamed.

21. The network node according to claim 20, wherein the content may be accessed by using a ticket.

22. The network node according to claim 20, wherein the streamed content is DRM protected content.

23. The network node according to claim 22, further comprising means for authenticating a DRM module in the second party terminal, confirming a right of the first party terminal to distribute the DRM content, manipulating the DRM content, if needed, to match the second party terminal, and creating a right specifically for the second party terminal to access the manipulated content.

24. The network node according to claim 23, wherein the means for manipulating includes means for decrypting the DRM content, reformatting the DRM content, if needed, to match the second party terminal, tagging the DRM content for the second party terminal, and re-encrypting the content with a specific key for the second party terminal.

25. The network node according to claim 22, further comprising means for generating a DRM module, and distributing the DRM module to the second party terminal.

26. The network node according to claim 19, wherein the network node and the first and second party terminals share a predetermined function, further comprising means for distributing a nonce to the terminals, and for deriving a content key based on the predetermined function, the nonce, and a session identity.

27. The network node according to claim 19, wherein the content is encrypted prior to storing.

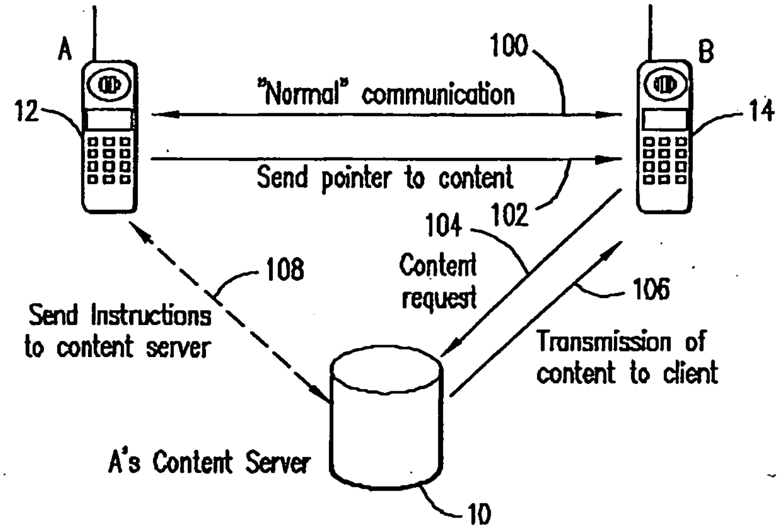


FIG. 1
(PRIOR ART)

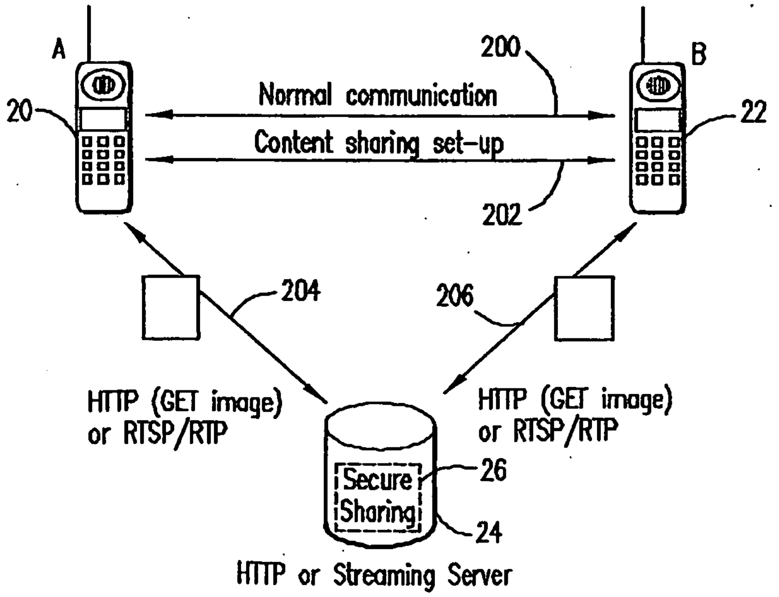


FIG. 2

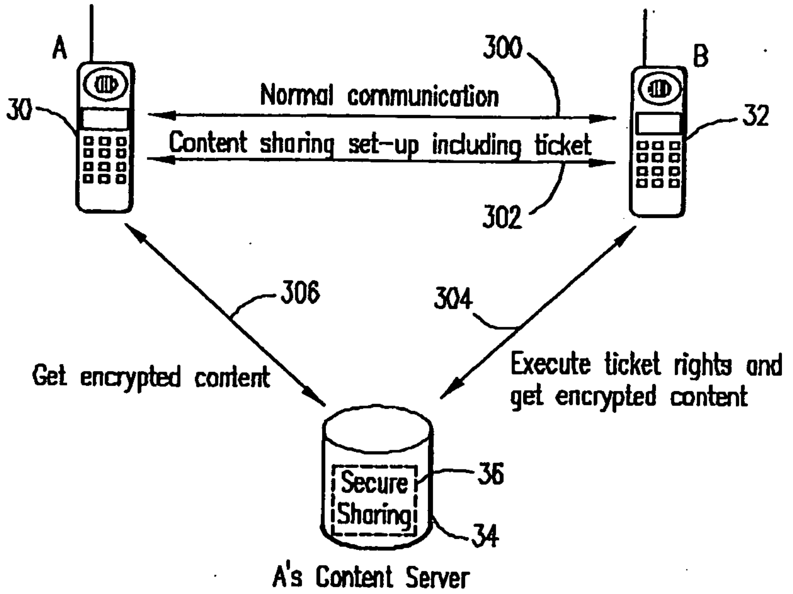

A
B
300
30
32
Normal communication
Content sharing set-up including ticket
302
306
304
Get encrypted content
Execute ticket rights and get encrypted content
Secure Sharing
36
34
A's Content Server

FIG. 3

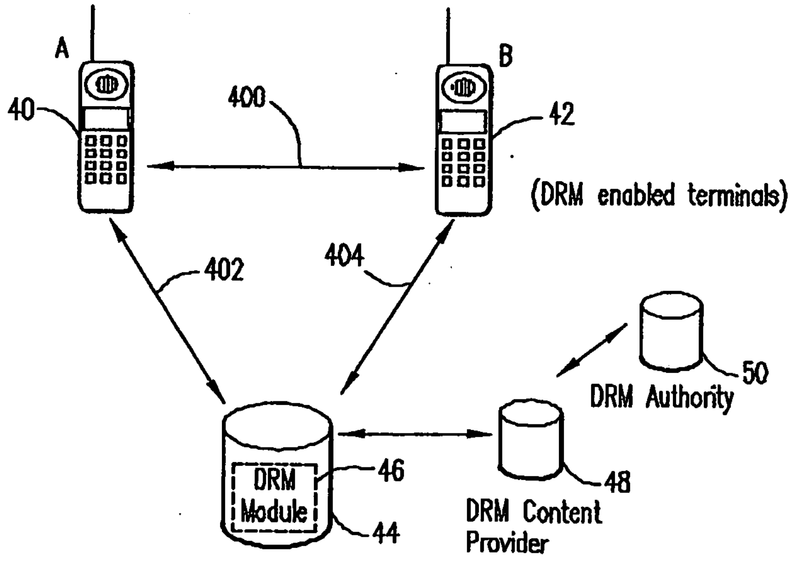

A
B
40
400
42
(DRM enabled terminals)
402
404
50
DRM Authority
DRM Module
46
48
44
DRM Content Provider

FIG. 4

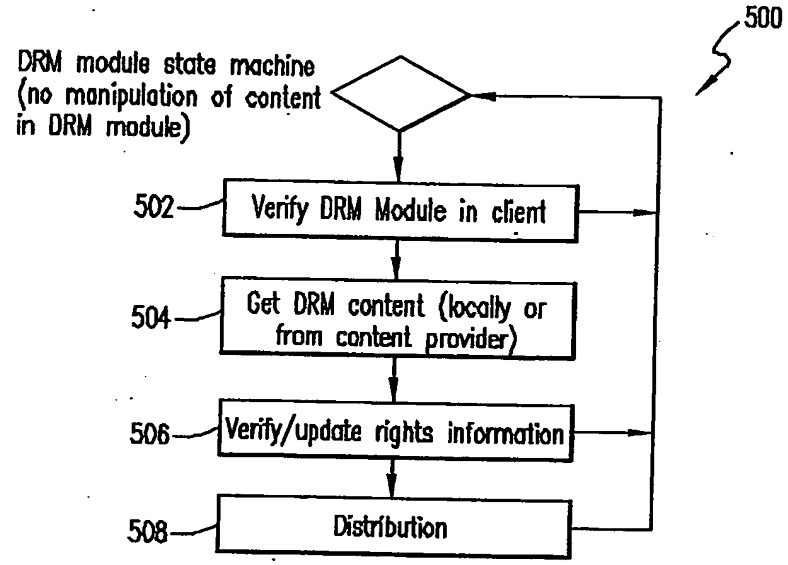

500
DRM module state machine (no manipulation of content in DRM module)
502
Verify DRM Module in client
504
Get DRM content (locally or from content provider)
506
Verify/update rights information
508
Distribution

FIG. 5

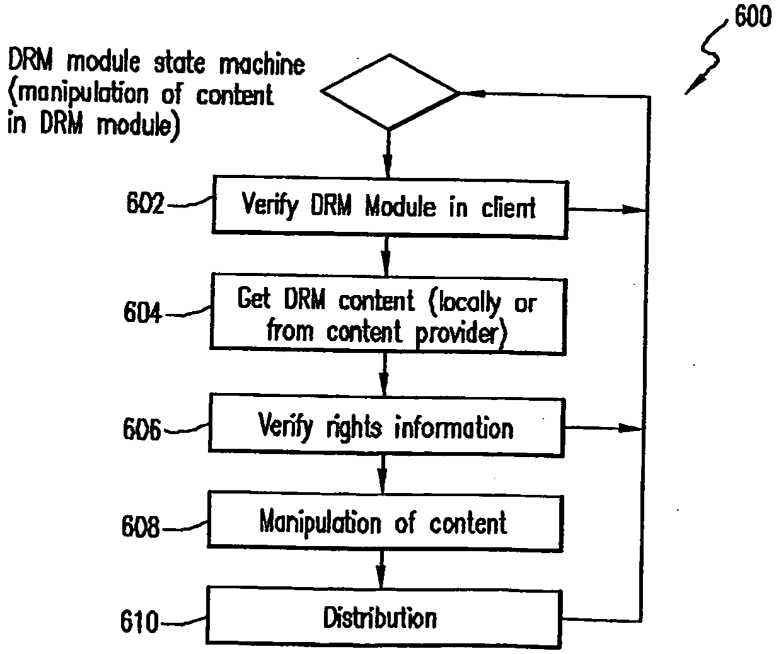

600
DRM module state machine (manipulation of content in DRM module)
602
Verify DRM Module in client
604
Get DRM content (locally or from content provider)
606
Verify rights information
608
Manipulation of content
610
Distribution

FIG. 6

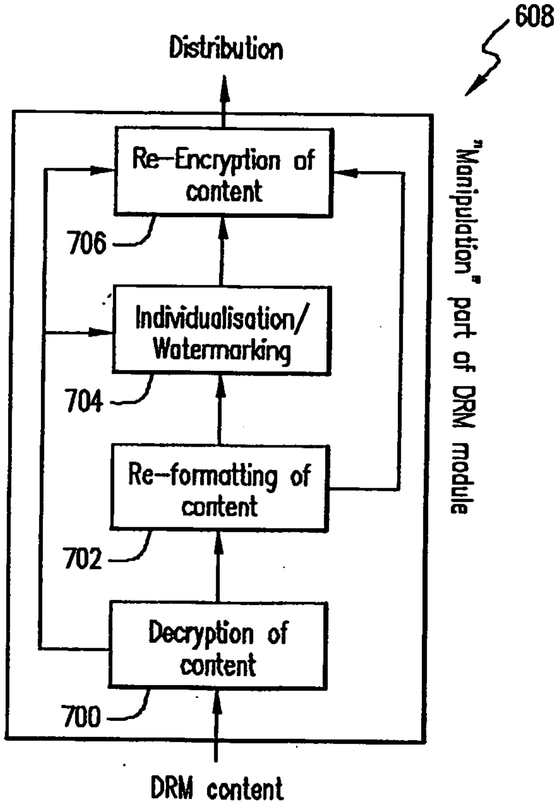

608
Distribution
Re-Encryption of content
706
Individualisation/ Watermarking
704
Re-formatting of content
702
Decryption of content
700
DRM content
"Manipulation" part of DRM module

FIG. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 03/00796

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 //H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 77775 A (LITAI ASSAF ;PELED ARIEL (IL); VIDIUS INC (US)) 18 October 2001 (2001-10-18) page 6, line 8 - line 30 page 7, line 23 - line 27 page 8, line 18 - line 25 page 9, line 9 - line 14; claims 1,6	1-3, 9-12, 18-21,27
Y		4-8, 13-17, 22-26

Y	WO 02 19628 A (CONTENTGUARD HOLDINGS INC) 7 March 2002 (2002-03-07) page 14, column 0046; claims 1-6	4-7, 13-16, 22-25

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search
4 August 2003

Date of mailing of the international search report
18. 08. 2003

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
NINA ÖDLING / ELY

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 03/00796

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2001/017885 A1 (ASAI ARITO ET AL) 30 August 2001 (2001-08-30) page 1, column 0008; claims 1,4,5 ---	4-6, 13-15, 22-24
Y	US 2001/009025 A1 (AHONEN PASI MATTI KALEVI) 19 July 2001 (2001-07-19) page 4, column 0084 ---	8,17,26
A	US 2002/002674 A1 (GRIMES TOM ET AL) 3 January 2002 (2002-01-03) page 2, column 0025 -column 0026 page 4, column 0040 -column 0041 abstract ---	1-27
A	WO 02 19653 A (IKIMBO INC) 7 March 2002 (2002-03-07) page 13, line 27 -page 14, line 4 page 18, line 17 - line 27; claims 1-4; figures 1,8 ---	1-27
A	US 2002/038425 A1 (KANNO SHIN-ICHI) 28 March 2002 (2002-03-28) abstract ---	1-3, 9-11, 18-20
A	EP 1 164 765 A (AT & T CORP ;AT & T WIRELESS SERVICES INC (US)) 19 December 2001 (2001-12-19) abstract ---	1-27
A	US 2002/013772 A1 (PEINADO MARCUS) 31 January 2002 (2002-01-31) page 1, column 0010 -page 2, column 0011 page 20, column 0272 page 21, column 0283 -----	8,17,26

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 03/00796

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
WO 0177775	A	18-10-2001	AU	5060201	A	23-10-2001
			CA	2406010	A1	18-10-2001
			EP	1279087	A2	29-01-2003
			WO	0177775	A2	18-10-2001
WO 0219628	A	07-03-2002	AU	8678801	A	13-03-2002
			WO	0219628	A1	07-03-2002
			US	2002108050	A1	08-08-2002
US 2001017885	A1	30-08-2001	JP	2001242786	A	07-09-2001
US 2001009025	A1	19-07-2001	GB	2364477	A	23-01-2002
			AU	2895801	A	31-07-2001
			WO	0154379	A1	26-07-2001
US 2002002674	A1	03-01-2002	AU	7170401	A	14-01-2002
			WO	0203604	A2	10-01-2002
WO 0219653	A	07-03-2002	AU	9059101	A	13-03-2002
			WO	0219653	A2	07-03-2002
			US	2002134083	A1	26-09-2002
US 2002038425	A1	28-03-2002	JP	2002108840	A	12-04-2002
EP 1164765	A	19-12-2001	US	2002026500	A1	28-02-2002
			EP	1164765	A2	19-12-2001
US 2002013772	A1	31-01-2002	EP	1271279	A2	02-01-2003
			JP	2003101526	A	04-04-2003
			AU	3007800	A	16-10-2000
			AU	3380900	A	16-10-2000
			AU	3381000	A	16-10-2000
			AU	3503900	A	16-10-2000
			AU	3608100	A	16-10-2000
			AU	3708700	A	16-10-2000
			AU	3710100	A	16-10-2000
			EP	1287636	A2	05-03-2003
			EP	1259863	A2	27-11-2002
			WO	0057684	A2	05-10-2000
			WO	0059150	A2	05-10-2000
			WO	0059151	A2	05-10-2000
			WO	0058859	A2	05-10-2000
			WO	0058810	A2	05-10-2000
			WO	0059152	A2	05-10-2000
			WO	0058811	A2	05-10-2000
			US	2003078853	A1	24-04-2003
			US	2002012432	A1	31-01-2002
			US	2002007456	A1	17-01-2002